

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(7) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 February 2002 (21.02.2002)

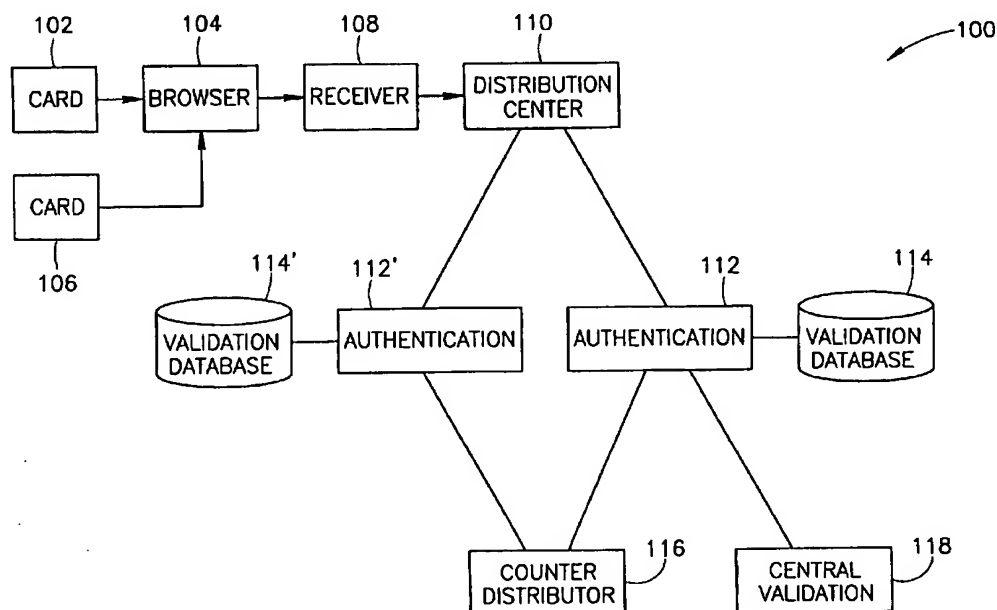
PCT

(10) International Publication Number
WO 02/14974 A2

- (51) International Patent Classification⁷: **G06F**
- (21) International Application Number: **PCT/IL01/00758**
- (22) International Filing Date: 14 August 2001 (14.08.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
137854 14 August 2000 (14.08.2000) IL
60/277,996 22 March 2001 (22.03.2001) US
- (63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 60/277,996 (CIP)
Filed on 22 March 2001 (22.03.2001)
- (72) Inventors; and
(75) Inventors/Applicants (for US only): **ANATI, Ram** [IL/IL]; Hactrog Street 16, Kfar Brandes, 38244 Hadera (IL). **ATSMON, Danny** [IL/IL]; Tayber Street 60, 53431 Givataim (IL). **SEGE, Alan** [US/US]; 1518 Euclid Street, Apt. 5, Santa Monica, CA 90404 (US).
- (74) Agents: **FENSTER, Paul** et al.; Fenster and Company Patent Attorneys Ltd., P.O. Box 10256, 49002 Petach Tikva (IL).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: MULTI-SERVER AUTHENTICATION



(57) Abstract: A method of transactional authentication, comprising receiving transactional information comprising: a card ID, a code and a counter at a first location, selectively transmitting said information to at least one of a plurality of authentication servers, applying a hash function to said information, and matching said hashed information to a database of hashes of valid information at a one of said plurality of authentication servers.



patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- *without international search report and to be republished upon receipt of that report*

MULTI-SERVER AUTHENTICATION RELATED APPLICATIONS

The present application claims the benefit of U.S. provisional patent application 60/277,996 filed March 22, 2001, titled "Method and system for remotely authenticating
5 identification devices", under 35 USC §119(e), the disclosure of which is incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates to authentication of cards for on-line transactions.

BACKGROUND OF THE INVENTION

10 Cards, in the bank-card form factor, are ubiquitous, and people everywhere use them for transactions and identification. Previously, people could only use those cards at dedicated machines such as ATMs and to make purchases at those stores that accept their cards. In a world where every Internet device is a point of sale, that is not enough.

Various types of transaction cards that generate a one-time code per transaction are
15 known, for example, smart cards. Typically, the code for a transaction is verified by a central location, which issues the cards.

SUMMARY OF THE INVENTION

An aspect of some embodiments of the invention relates to distributing the authentication of a transaction performed using a transactional card. In an exemplary
20 embodiment of the invention, an authentication of a code generated by the card is performed by one of several distributed authentication servers, for example based on availability or on affiliation of the authentication server with a transaction manager.

An aspect of some embodiments of the invention relates to performing at least some of the authentication of a transactional card using an authentication server that is not affiliated
25 with a card issuer. In one exemplary embodiment of the invention, the authentication of a card is by a card producer (which is not a card issuer) or by a third party authenticator. Alternatively, a single card may be "issued" by several card issuers, each of which may selectively authenticate a transaction.

An aspect of some embodiments of the invention, relates to a database for a distributed
30 authentication server, in which only hash functions of authentication data is stored. Thus, if such a server is broken into, there is no data available to be stolen. Optionally, each such server may add its own level(s) of authentication, for example, passwords.

In an exemplary embodiment of the invention, the contact with the card holder is via a WWW page into which the card holder enters the transactional information. In an exemplary

embodiment of the invention, a single software unit, for example an ActiveX element is used for a plurality of different authentication servers.

An aspect of some embodiments of the invention relates to a transactional card that can emulate a plurality of different cards provided by different card issuers. In an exemplary embodiment of the invention, the card generates a single code that is selectively authenticated by only one card-issuer associated authentication server. Alternatively or additionally, the card can selectively generate information for a plurality of card issuers. Possibly, the card real-estate reflects the current programming/emulation ability of a card.

An aspect of some embodiments of the invention relates to dividing up authentication functions between a plurality of locations and computers, including one or more of:

- (a) safety rules (e.g., is card being used in an abnormal manner;
- (b) validity of card number;
- (c) validity of code information;
- (d) validity of counter used to generate code information; and
- (e) password information.

In some embodiments of the invention, even a single authentication step is performed by two different computers, separately, or together. Alternatively or additionally, for some transactions, not all authentication levels are performed. Optionally, the number of partial authentications and/or their total sum is tracked.

BRIEF DESCRIPTION OF THE DRAWINGS

Particular embodiments of the invention will be described with reference to the following description of preferred embodiments in conjunction with the figures, wherein identical structures, elements or parts which appear in more than one figure are preferably labeled with a same or similar number in all the figures in which they appear, in which:

Fig. 1 is a block diagram of an authentication configuration, in accordance with an exemplary embodiment of the invention;

Fig. 2 is a schematic illustration of a transaction card, in accordance with an exemplary embodiment of the invention;

Fig. 3 is a schematic side illustration of a modular switch, in accordance with an exemplary embodiment of the invention;

Fig. 4 is an overview of an exemplary process of ComSense card authentication, in accordance with an embodiment of the present invention;

Fig. 5 illustrates the process of key generation, management, and the creation of hash databases bearing a one-to-one relationship with the set of one-time codes that each card is capable of transmitting, in accordance with an embodiment of the present invention;

Fig. 6 illustrates the interrelationships of the system components of the ComSense solution for Issuer, in accordance with an embodiment of the present invention;

Fig. 7 is an illustration of the system data flow, in accordance with an embodiment of the present invention; and

Fig. 8 is a schematic illustration of an exemplary system architecture, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

Fig. 1 is a block diagram of an authentication configuration 100, in accordance with an exemplary embodiment of the invention. A card 102 sends transaction information to a browser 104. The transaction information is decoded by a receiver 108, which may or may not be part of the browser. Optionally, the receiver and the browser are on a same computer, however, this is not required. A distribution center 110 receives the information from receiver 108 and sends the transactional information to an authorization server 112, which compares the transactional information against information stored in a local validation database 114. It is a particular feature of some embodiments of the invention that a plurality of possible authentication servers 112 and 112' are available.

Card 102 maybe any type of transactional card, for example an acoustic card that communicates with a computer via its microphone, such as described in PCT publications WO 00/21020 and WO 00/21203 and in US patent application filed May 12, 2000, attorney docket 20257-11, by applicants Alon Atsmon, et al., and entitled "Physical Presence digital Authentication System", the disclosures of which are incorporated herein by reference. Alternatively, other transactional means are used, for example, cellular telephones, smart cards and devices using bluetooth communication, such as palm computers. Alternatively or additionally, such electronic devices may function as card readers. Alternatively, the transactional information may be electronic, for example, various forms of electronic cash. The connection may be one directional (only card to computer) or two directional. Although a browser-based embodiment is described, a transactional card may be operated over telephone lines or using dedicated software, for example.

In an exemplary embodiment of the invention, the card generates a one time code, using a counter-based random number generation function. Alternatively or additionally, card 102 generates a digital signature for a transaction content and/or time and/or vendor.

In an exemplary embodiment of the invention, receiver 108 comprises an ActiveX type software module or a Java applet that forms part of a WWW page through which the transaction is being performed. Optionally, a single applet is used for a plurality of different pages and/or card issuers, for example being downloaded from a central source or being
5 provided locally on the computer. Alternatively, a stand alone acoustic recognition software may be used instead.

In some embodiments of the invention, no distribution server 110 is provided, for example, receiver 108 sending the information directly to a predetermined authentication server (or only one provided, or only one being relevant) or distribution server 110 being
10 integrated with receiver 108 and/or browser 104. In some embodiments of the invention, the determination which authentication server to send to is dependent on the contents of the WWW page, on the card ID or on other information entered at browser 104 (e.g., via an "other" input 106) and/or on the information transmitted by the card.

The transaction information from card 102, may include, for example, one or more of
15 the card ID, a counter count, a code generated using the counter and/or information entered using the card. Alternatively or additionally, a user may provide additional transactional information, for example, by entering it using other input 106 (e.g., a keyboard and/or a mouse) or the information may be acquired from the WWW page, for example an amount or a vendor identification. Possibly, such information is tagged in an HTML file used for
20 displaying the page or transmitted when a submit button on the page is activated. In some embodiments, card 102 may act as a submit button. Additional transactional information may thus be added by one or more of card 102, other input 106, browser 104, receiver 108 and distribution center 110.

A plurality of authentication servers 112 maybe desirable for several reasons, for
25 example, one or more of:

(a) providing geographical local and/or fast authentication, especially for world wide use of cards in which the code has a limited validity time;

(b) providing redundancy, in case a server fails;

(c) providing vendors and/or card issuers with personal authentication services; and

(d) providing load balancing of CPU and communication resources.
30

In some embodiments of the invention, authentication server 112 validates the transactional information using validation database 114. In an exemplary embodiment of the invention, the validation is by comparing the transactional information to information in database 114. Optionally, database 114 a hash of the original information, rather than the

information itself. Thus, if database 114 is hacked into, it cannot yield the authentication information. In an exemplary embodiment of the invention, an MD5 type hash function is used. As used herein, a hash function is a function that maps original information into an indecipherable sequence of symbols. In some cases a real hash function is used, characterized
5 in that no reverse hashing can be performed. Alternatively, a reversible hashing is used, for example, public key encryption. In these embodiments, a decryption key may be stored at database 114.

In an exemplary embodiment of the invention, database 114 contains, for a plurality of cards, a plurality of codes matching a plurality of counter values and, optionally card IDs.
10 Alternatively or additionally, database 114, or an additional database may include other authentication information, such as a password entered using other input 106. Possibly, other input 106 comprises a biometrics input, such as a retina reader or a fingerprint detector. If database 114 is for time-stamped codes, the database may include a plurality of codes for the different times. In one example, a record is stored for each card at time steps of one minute.

15 Different databases 114 may use the same hash or they may not. Thus a same card may be authenticated against different data in different authentication servers. Conversely, the choice of a hash function may determine which authentication server 112 can perform the authentication.

Hashing of the transactional information may be performed at one or more of: card
20 102, browser 104, receiver 108, distribution enter 110 and authentication server 112.

In some embodiments of the invention, a check for the validity of the counter used to generate the transactional code is also performed, for example at authentication server 112 or at a central validation center 118. A counter distributor 116 may distribute current and/or update values of counters (or corresponding data records) between the authentication servers,
25 to keep them up to date. Optionally, the counter validation is only performed to see if the counter is within a small number of counts from a previously known value. If the counter is outside the range, a special request to counter distributor 116 may be performed. Optionally, counter values are pre-fetched to localities where activity of a particular card is detected, for use in expected further activations of the card.

30 Additional validation steps may be performed at one of the above validation and authentication servers or at a separate additional authentication server, for example at a separate password authenticator (not shown). Alternatively or additionally, the above described authentications, may be divided among the available authenticators in various ways, for example varying the location and/or level of authentication.

Optionally, different levels of authentication are required for different activities, for example, low cost or security activities (e.g. viewing a WWW page) may only require presenting a valid card ID, while higher cost activities (e.g., modifying information) may require code validation, counter validation and/or entering a password. In another example, if a purchase is being sent to a user's home, optionally no counter validation is required. Changing the home address, may require such validation. Possibly, connections from home require a weaker authentication than connections away from home, for example, an additional password or a less-likely to be overcome hash function. Optionally, the card includes the ability to selectively advance the counter or not. Alternatively, a counter validation may be based on a series of correct counters being presented by the card, indicating that it is the true card.

In some embodiments of the invention, a time stamp is used, alternatively or additionally to using a counter. A card 106 may include a clock. Alternatively, the card may retrieve the clock, or other limited duration information, from browser 104, receiver 108, distributor 110 or authentication server 112. The validity of a time stamped content may be checked, using a suitable entry in database 114. Possibly, database 114 includes entries corresponding to a small number of transaction amounts.

As noted above, different authentication servers may be provided to different card issuers, even for a same card. In an exemplary embodiment of the invention, databases 114 are limited to represent only those cards that are currently (and/or expected to be) in the jurisdiction of authentication server 112. Thus, one card can only be authenticated by only one server, while another card can be authenticated by two servers.

As noted above, a physical single card can be issued by a plurality of card issuers. Various methods may be implemented to differentiate between the card issuer to be used for a particular transaction. In one example, the transactional information, for example entered (or pre-set) on a WWW page may determine the issuer. In another example, a single physical card may transmit a different code to represent cards by different emulated card issuers. In another example, a card transmits a series of different IDs for different issuers. In another example, one of the elements along the line between browser 104 and authentication server 112 converts a card ID into a card issuer ID, for example using information provided by the user or by the card issuer. In another example, a user may set rules for card issuer selection. In another example, multiple activations of a card are used to represent different card issuers, for example, by receiving a number of consecutive codes by receiver 108. Alternatively, the card may transmit different codes depending on a length or number of presses of a switch on the card. In another example, the first card issuer to respond to an authentication request, or a card

issuer that charges a lowest cost overhead is selected. The charge amount may be transmitted only after a card issuer is selected. In this example, the authentication may be performed by a central server.

In one exemplary embodiment of the invention, a single card ID is registered with one or more card issuers. Alternatively or additionally, the card ID is linked to the card issuer ID, but is not registered. Registration allows the authentication server to recognize the card as belonging to an issuer. Alternatively or additionally, hardware or software modification of the card (or controls on the card) enables such registration and/or otherwise controls the codes sent by the card and/or the type of distribution effected by distributor 110 and/or type of authentication by authentication server 112 and/or other authentication or validation servers.

It can thus be appreciated that a single physical card may be required to emulate a plurality of credit card issuers. A potential property of such a card is that the card does not belong to a credit card company. Thus, the utilization of real-estate on the card surface may be more flexible. Alternatively or additionally, the card may not conform to all credit card design standards.

In an exemplary embodiment of the invention, a card 102 can be programmed, for example acoustically (e.g., for an acoustic card) or via smart card contacts or RF radiation, to include the required emulation for the various card issuers.

Fig. 2 is a schematic illustration of a multiple endorsement transaction card 200, in accordance with an exemplary embodiment of the invention. Card 200 comprises a body 202 having one or more standard card features, such as a number area 204. Unlike standard cards, card 200 includes a plurality of endorsement areas 206, 208, 210, 212 and 214; any number of such areas may be provided.

Once card 200 is programmed to emulate a particular card type, a suitable sticker may be provided, for example, by mail, to place in an endorsement area. Optionally, the endorsement areas are depressed, so the sticker does not affect the thickness profile of the card. Alternatively, the width variations may be limited to areas where the card does not affect the expected card functionality (e.g., ATM machine). A sticker may be removable or it may be designed to be damaged when removed. It should be noted that the card packaging can vary, for example, if the card is emulated by a cellular telephone or a smart card.

Alternatively to a sticker being function-less, a sticker may modify the behavior of card 200. In one example, an endorsement area 210 includes two or more contacts 216, two or more of which are shorted by the back of the sticker (if placed correctly). The shorting of the contacts may identify the endorsement on the face of the sticker and/or may determine

hardware functionality and/or transmitted codes of card 200. The shorting may be pattern-less, for example using a conductive adhesive on the back of the sticker. Alternatively, the sticker may contain a patterned conductive area, for example to selectively short only certain ones of contacts 216. Alternatively or additionally, the sticker may sit on smart-card style connectors of the card.

Alternatively or additionally, the "sticker" may include electronics, for example a capacitor, a resistor or a ROM, for programming the card. Alternatively or additionally, the sticker may include a code generating circuitry, with card 200 serving as an amplifier for generating an output signal.

Alternatively or additionally, to conductive coupling, the sticker may affect the capacitance or the inductance of the connection between the electrodes. Alternatively or additionally, the sticker may be magnetic, and affect a reed-switch embedded in card 200. Alternatively or additionally, other contact-less coupling methods known in the art may be used.

Alternatively or additionally, to a sticker, a display (not shown), such as an LCD display may be used to display endorsements.

In an exemplary embodiment of the invention, card 200 includes a switch (not shown) for sending the above transactional information. Optionally, a plurality of switches are provided, one for each endorsement. The switches may be, for example, on an opposite side of card 200 from their respective endorsement. Possibly, a switch is not functional if a sticker is not placed in its respective endorsement area.

Possibly, the sticker itself functions as a switch, selectively shorting (or otherwise affecting the electrical behavior) of contacts 216.

Fig. 3 is a schematic side illustration of a modular switch 300, in accordance with an exemplary embodiment of the invention. Switch 300 comprises a base 302 and an upper portion 304 separated from base 302, such that when pressure is applied to upper portion 304 an electrical short is formed between base 302 and upper portion 302. A resilient filling may be provided between the two switch parts. Alternatively or additionally, the contact is formed between the center of portion 304 and base 302. Optionally, base 302 has an adhesive bottom, for attachment to card body 202.

In an exemplary embodiment of the invention, one or more spikes 306 are formed on the bottom of base 302 such that when base 302 is brought against card body 202, the spikes penetrate into card body 202 and complete an electrical contact. Thus, contacts 216 (Fig. 2)

can be coated with a protective layer against accidental electrical contact. Such a spike arrangement may also be used for stickers that close contacts, as described above.

In an exemplary embodiment of the invention, switch 300 generates a "click" sound when pressed. Alternatively or additionally, card 200 generates an audible feedback prior to or after an ultrasonic coded signal is sent to browser 104 from card 102. Alternatively or additionally, the feedback is from receiver 108. In some embodiments of the invention, activating the card generates a feedback by virtue of causing browser 104 to download a WWW page, for example a shopping page. Such a page can be navigated using a single switch, for example, by allowing only one activity at any point or by distinguishing single and double depressions of the switch. Such depressions do not usually require an in-depth authentication, however, a counter update may be provided to counter distributor 116. Alternatively, the counter may advance only every few depressions and/or after even only one depression if a sufficient time (e.g., 2 minutes) elapsed.

Following is a technical description of a particular implementation of the above described invention. It is noted that the elements and acts in the following described implementation are not all essential for carrying out the invention.

In an exemplary embodiment of the invention, cardholders can use their cards to (i) "Launch" their online account or other personal services from a PC bearing our persistent client; (ii) "Authenticate" to those same services from anywhere using a web-based client; and (iii) "Transact" in conjunction with an Issuer's merchant partners or preferred third-party form filling service.

Fig. 4 is an overview of an exemplary process of ComSense card authentication, in accordance with an embodiment of the present invention.

Hardware

Card specification

One exemplary feature that differentiates the instant card, in some embodiments of the invention, from an ordinary bank card is the flat button embedded in the corner of the card. This button is a switch, which the user squeezes between two fingers—typically the thumb and forefinger—to activate the card.

The exemplary card features the following technical characteristics:

Card Feature	Description
Transmission speed	Approximately 200 bits per second from card to PC
ISO standard magnetic stripe	HiCo, or other industry standard
Card lifespan	Up to 10,000 operations (approximately two years)

Dimensions	0.76 by 85 by 54 mm corresponding with the ISO standard
Robustness	Sustains bending and torsion. Highly resistant to electromagnetic radiation.
Range	3-6 inches from microphone

Manufacturing

The card is optionally manufactured to comply with the requirements of the relevant portions of ISO 7810, ISO 7811 and ISO 7816. The ComSense electronic module is delivered to a Visa certified card manufacturing facility where it is further processed into a card. The plastic sheets containing the appropriate graphics and logos will be produced in this facility utilizing industry standard materials and processes and under the controls of a Visa certified security system.

The ComSense electronic modules will be laminated within the plastic sheets. Following lamination, the cards will be singulated and electrically tested. The cards will then be further processed utilizing industry standard equipment and processes. That certified facility will attach holograms and signature panels and will transfer the cards into Issuer's possession for secure shipment to the designated personalization facility.

At Issuer's discretion, the cards can then be embossed and programmed utilizing industry standard processes and equipment. While embossing practices and specifications vary somewhat, the embossable area will likely be slightly reduced, as compared to most standard credit cards, due to the presence and layout of electronic components within the current card design.

Key management

ComSense will have keys generated for the cards.

ComSense will provide Issuer with a one-way, MD-5 hashed database of calculated transmissions per card. ComSense will transfer that database to the location of the Authentication Server; namely, where the OLA servers are hosted.

Fig. 5 illustrates the process of key generation, management, and the creation of hash databases bearing a one-to-one relationship with the set of one-time codes that each card is capable of transmitting, in accordance with an embodiment of the present invention.

ComSense Software

The ComSense solution for Issuer involves a hybrid scheme that combines web-based software and client-based software. Specifically, the scheme involves:

- Integrating **transient clients** (ActiveX for IE; Java applet for Netscape) in a Issuer login page and elsewhere on the Issuer website, as desired.

- Installing **persistent client or “tray” application** upon running the ComSense Install wizard.

The transient client provides control of card reception as a web-based service. This capability enables cardholders to use their card from any computer that is equipped with an operational sound system, microphone and connected to the Internet—even if the computer does not have the ComSense software installed as a tray application.

The persistent client application provides an auto-launch feature and one-click access from trusted platforms.

Due to the web-based capability, running the Install wizard is not mandatory to using the card. However, we strongly recommend that users do run it, as it includes tests that determine if the card and microphone are functioning properly.

System architecture

Fig. 6 illustrates the interrelationships of the system components of the ComSense solution for Issuer, in accordance with an embodiment of the present invention.

Server and database software

The server can run, for example, under WindowsNT, Sun Solaris operating system, or some other operating system to be requested by Issuer. The card transmission database can run, for example, under Microsoft SQL.

The following events take place on the server, when the Issuer user operates the card to log onto Issuer services:

1. The user activates the card in conjunction with the tray application or with the transient client included in the Issuer login page. In either case, the client PC receives the card's transmission.
2. The PC then sends the signal in its original encrypted form (i.e. plain card serial number and encrypted counter + card-specific second serial number) to the Authentication Server.
3. The server, which resides in a secured location, uses the card serial number to query the hashed list of the card's possible transmissions.
4. The server then compares the counter with the previous counter (the current counter must be greater than the previous counter).
5. If the counter meets these requirements, the system considers the card valid. Otherwise, the card is considered invalid.
6. The server updates the counter value so that the system is prepared for the next authentication request emanating from that card.

Please note the following optional points regarding the system's architecture:

- The Authentication Server is an independent component in the overall architecture of the system.
- At no point during the authentication process do any of the machines that make up the system architecture know or use the secret ciphering keys. In fact, the keys do not exist in any of the machines within the system architecture.
- The Authentication Server may reside on the same Intranet as the Issuer servers; therefore, the data that transfers between the servers is internally safe.

Fig. 7 is an illustration of the system data flow, in accordance with an embodiment of the present invention.

Registration

Issuer can design and implement a web-based interface that handles card registration for online verification and authentication. Issuer can also be responsible for managing user registration status. Thus, Issuer can therefore be responsible for managing all aspects of the registration process, including preventing duplicate or false registrations.

The Authentication Server can, as a minimum, validate a ComSense card but not associate the card with any other data. The Authentication Server perceives a card to be active and valid from the moment its unique transmissions database is appended to the card's database.

Communications layer

ComSense will provide Issuer with its communications receiver layer to implement on an Issuer Card web-based services login page. The communications layer can, for example, support both MS Internet Explorer (version 4.0 or higher) and Netscape's Communicator (version 4.06 or higher). The communications layer comes in two versions: ActiveX for IE users and a Java applet for Netscape users. The communications layer receives the transmission from the card and sends it to the authentication server. Both versions of the communications layer can come with a graphical user interface. In either form (transient or persistent), the client will authenticate to a specific predefined Issuer/Issuer websites or Internet services specified by Issuer. ComSense can modify the comm layer to additional Issuer/Issuer services as requested.

Retrieving card serial number

ComSense will provide Issuer with an interface for extracting the card serial number from a given card transmission, so as to allow for parallel processing of data and avoiding possible bottlenecks in Issuer's implementation of business rules. Through this interface,

Issuer will receive a given card's serial number as soon as it enters the system and even before the system sends that number to the Authentication Server.

Auditing: server-side

According to guidelines provided by Issuer, ComSense software will include logging features for collecting data related to user login and transactions. The software may include logging of at least the following data: Timestamp(date and time), Card serial number, Card signal (transmitted data), Card counter, IP address of the requesting machine, Authentication result. Issuer will correlate that data with data from its transaction system to cross-reference when a card is operated to effect a transaction, and the size of that transaction and resulting interchange fee. This information can be used to calculate the Incentive payments due ComSense.

In some embodiments of the invention, at no time will the ComSense software knowingly collect user data that is not relevant to the applicability of the software. The resulting traffic database will belong to ComSense Technologies Ltd. As agreed by the two parties, ComSense will periodically obtain an electronic copy of the database. Issuer will also share with ComSense other relevant data collected by Issuer's login and transactions logging systems and, in particular, data that relates to how often users enter Issuer services with or without using the ComSense card. From time, to time, Issuer may also collect data from cardholders relating the card's effectiveness and usability that ComSense might find useful for future product enhancements or marketing. Alternatively, ComSense will collect the data and distribute it to the issuer.

Implementing by Phone

Note that certain advantages obtain when the cards are used transmitting a signal in the acoustic range on a POTS phone or cell phone system. Notably, since the customer premises equipment ("CPE" or phone handset or mobile phone) always conducts sound over the wires whenever it is on, our comm layer can reside at a central location, and just detect and process card transmissions there.

In the case of a POTS implementation, that comm layer can reside in a number of central locations in the phone network. For example, in order of their distance from the CPE, the comm layer can reside on equipment at the local POP, at the Interlata or interexchange connection point, at the equipment location of the carrier providing toll free service, at the call center maintained by the service associated with the phone number dialed. The comm layer could also be housed in CPE equipment itself. That would allow individual callers to authenticate themselves for secure conversations.

Using bi-directional, two cardholders could each simply hold their cards up to their handsets. One cardholder would activate his card, and the other would receive the transmission remotely over the phone. This method is ideal for exchanging information quickly by phone such as contact information, or for authenticating for conference calls or other private and secure communications.

Cellular phones present a special opportunity. The comm layer can be stored in any of the places discussed above for POTS, giving the same functionality as for POTS phones. But housing the comm layer at each of two additional locations gives rise to other sets of card applications.

Comm Layer housed at a server, such as the voice dialing server. Many cellular phone systems now offer voice dialing. Often, that functionality is largely server-based. Activating the phone immediately establishes a connection with a server hosting voice dial functionality. In that environment, housing the comm layer at the server allows the cardholder to open or activate his phone, and then activate the ComSense card when prompted to speak a name for voice dialing. The server/comm layer would receive the card transmission, and take appropriate action.

Those actions could include without limitation (i) looking up the phone number associated with the card service and then dialing the number; (ii) looking up the wireless web service associated with that card, and launching and logging into that service on the customer's cell phone. Some of the advantages obtaining from storing the comm layer at the voice dialing, or other cell phone system central server are that (i) the cell phone handset equipment would require no if any modification; and that (ii) since only a single database service would need to be kept up to date, the system would always support all issued cards whose functionality had been entered into a functionality database (phone numbers, websites associated with each card.) Optionally, the comm layer could also be housed in the cellular phone itself, making card functionality available even when the phone is out of range or "roaming."

The information flow in such a cellular system can be as follows:

1. Card activation making a one-time-code modulated on a sound signal.
2. Sound signal reaches cell phone
3. Sound signal carried from phone to cell, and from cell to a central server, such as a voice dialing server
4. Sound signal demodulated, to reveal the one-time code
5. One time code processed to identify the card, but not necessarily to authenticate it
6. Affiliated WAP or website, or phone number, identified in a central card database

7. New signal instantiated, and sent to phone to dial that number or activate website on the phone,
8. Simultaneously, a signal with the card's one time code is sent to that website or phone number, where the code is authenticated, for example using the hash database lookup method described above..

The user is authenticated by the service, which is by now in direct communication with the cell phone. The user receives personalized web content, or instructions over the dial-up service


Client software

Feature	Description
Operating system	Windows 95, 98 Windows NT4, 2k
System requirements	Pentium 100Mhz, 32 Mb RAM, 1 Mbyte free space on hard disk; sound card
Browsers	Microsoft Internet Explorer 4.0 or higher; Netscape Communicator 4.06 or higher AOL browser versions 4 or higher

Tray application

ComSense provides a single tray application that, after installation, runs automatically each time the user turns on the PC and Windows opens.

Installing the tray application software is a short and easy process. During installation, the Install wizard prompts the user to validate his/her card. This process, if desired by the user, establishes the installed computer as a "trusted platform" for the unique card (and unique user). Once installed, the ComSense tray application enables the cardholder to use the card to gain quick and secure access to Issuer's Issuer services.

Once the software is installed, a ComSense-branded tray icon (, or another logo) appears in the Task Bar to indicate that the ComSense application is active. Each time the user activates the ComSense card, this tray icon changes color (currently from yellow to green, and back to yellow shortly thereafter). The user can disable the software at any time.

The software optionally includes an "uninstall" feature.

The user activates the card by squeezing the card's embedded button. The ComSense tray application then validates the card's transmission. If a transmission is valid, the

application performs one of the following:

- **If the browser is closed:** On a trusted platform, the application launches the browser, opens the predefined, auto-launch Issuer website, and logs in the user. On a not-trusted platform, after activating the card, the user will also supply his/her password.

- 5 • **If the browser is open but is not displaying a web page from the predefined, auto-launch Issuer domain:** In the case of a trusted platform, opens a new browser window, opens the predefined auto-launch Issuer website, and logs in the user. In the case of a not-trusted platform, after activating the card, the user will also supply his/her password.

10 Note that the need to present a physical card and provide a password to authenticate oneself is the same authentication norm as used by ATMs.

If a transmission is invalid, the user receives an appropriate message and/or instructional feedback.

Auditing: client-side

15 To ensure efficient logging, the ComSense solution captures the user's request as soon as it is made. This auditing process is conducted in the same manner as--and in addition to--auditing on the server-side.

Security scheme

20 The ComSense card provides secure access and transactions on the web. The card transmits one-time codes and a card serial number. Upon determining that a valid transmission has taken place, the application forwards the card transmission to the ComSense Authentication Server. The server uses an MD-5 one-way hashed database of all cards and their possible valid transmissions for card verification and authentication. At no point during the authentication process do any of the machines that make up the system architecture know or use the secret ciphering keys. In fact, the keys do not exist in any of the machines within the system architecture.

Implications of the security scheme:

- Each ComSense card is unique. Different cards enable access to different accounts.
- A hacker/virus will not be able to get the card's serial number by "looking" at the user's hard disk, since the card's serial number is not stored there. The card serial number is also not stored in the application's .exe file.
- 30 • Even if someone records one or more of the card's transmissions and tries to re-transmit them later, the intruder will not gain access because the software accepts only

one-time codes that have a counter higher than the counters previously transmitted. The intruder will not be able to isolate counter data within the transmission (a hacker attack known as a "replay attack") because this data is encrypted together with other parts of the message.

- Knowing a user's name and card serial number will not enable another individual to access the user's online private account.
- No software element in the system holds the secret cipher keys. No machine in the system knows or uses the secret ciphering keys.
- The authentication server holds an MD-5 hashed database. This means that, even in the unlikely event of the database being acquired by an unauthorized party, it is virtually useless. The card cannot be used outside the system.
- The user's full record of personal details is not stored on the ComSense server, in the user's machine, or on the ComSense card.

Multiple Authentication Network.

This system can be modified to allow the same card to authenticate to multiple services. Instead of just one, multiple hash databases are created for each card, corresponding to a different hash function in each case.

Now consider when two different servers house two different hash databases corresponding to the same card. Each is able to conduct its own authentication of the card, without sharing any information. Optionally, each server must somehow update the other as to the most recent counter value that it has received, so that each can conduct proper authentication of the single card next time. One method of synchronizing the two server's status as to the counter value would be to maintain a separate but central database that always carries the updated value of each card counter in the system.

Fig. 8 is a schematic illustration of an exemplary system architecture, in accordance with an embodiment of the present invention.

Exemplary Card Graphics

ComSense will manufacture the Issuer cards with the same graphical design as that of previously distributed Issuer cards. In addition, the cards will contain the ComSense-branded button and logo, as illustrated below:

- The button will be of a fixed size, occupy a fixed location on both sides of the card, and have graphics that mark it as a point that the user needs to squeeze.

- The ComSense logo will appear in one place on the front and back of the card, at the location of the switch.

The present invention has been described using non-limiting detailed descriptions of embodiments thereof that are provided by way of example and are not intended to limit the scope of the invention. It should be understood that features and/or steps described with respect to one embodiment may be used with other embodiments and that not all embodiments of the invention have all of the features and/or steps shown in a particular figure or described with respect to one of the embodiments. Variations of embodiments described will occur to persons of the art.

It is noted that some of the above described embodiments describe the best mode contemplated by the inventors and therefore include structure, acts or details of structures and acts that may not be essential to the invention and which are described as examples. Structure and acts described herein are replaceable by equivalents which perform the same function, even if the structure or acts are different, as known in the art. Therefore, the scope of the invention is limited only by the elements and limitations as used in the claims. When used in the following claims, the terms "comprise", "include", "have" and their conjugates mean "including but not limited to".

CLAIMS

1. A method of transactional authentication, comprising:
receiving transactional information comprising: a card ID, a code and a counter at a
5 first location;
selectively transmitting said information to at least one of a plurality of authentication
servers;
applying a hash function to said information; and
matching said hashed information to a database of hashes of valid information at a one
10 of said plurality of authentication servers.
2. The method of claim 1, wherein said counter is updated at a counter server distinct
from said one or said plurality of authentication servers.
- 15 3. The method of claim 2, wherein said authentication server(s) check said counter server.
4. The method of claim 1, wherein said counter comprises a time stamp.
5. The method of claim 1, wherein said code is different for each authentication.
- 20 6. The method of claim 1, wherein said transactional information is modulated and
received by means of acoustic signal.

1/7

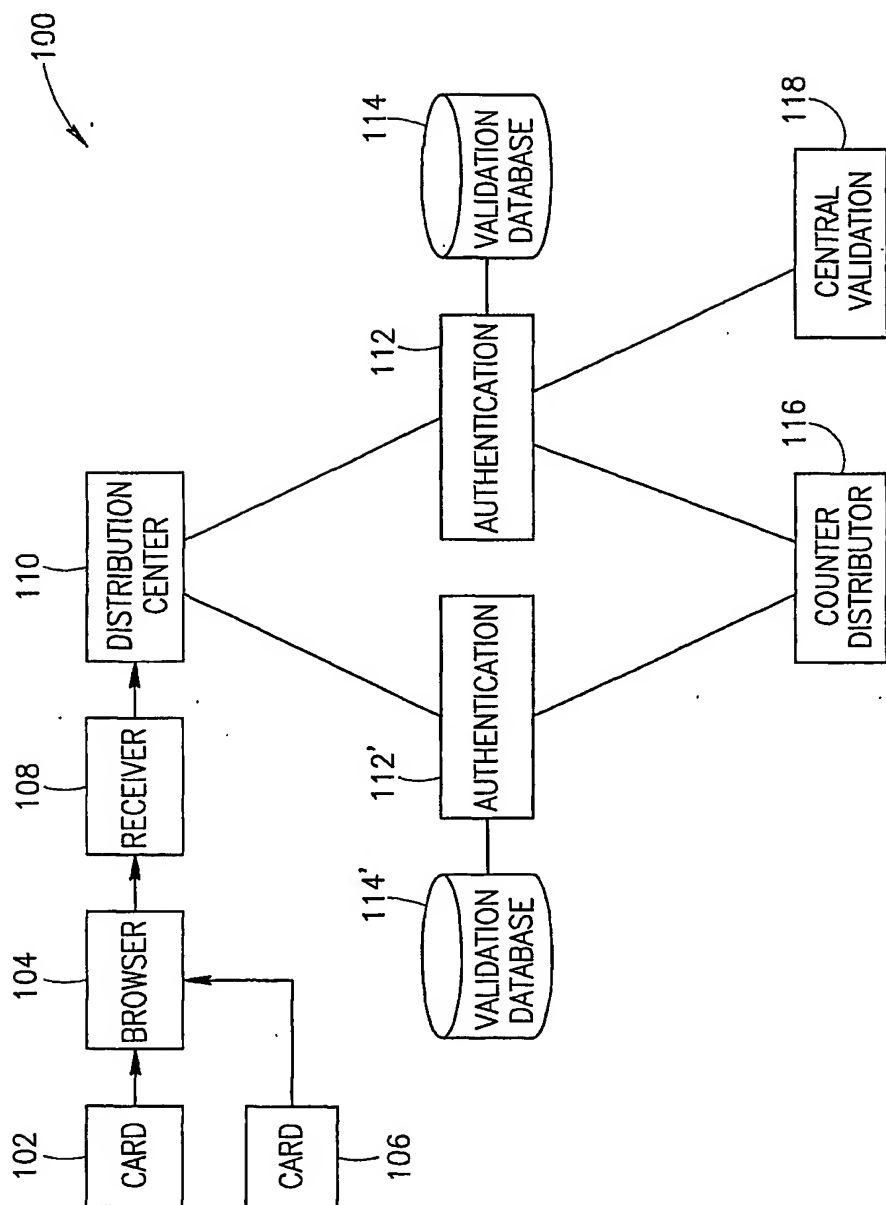


FIG.1

2/7

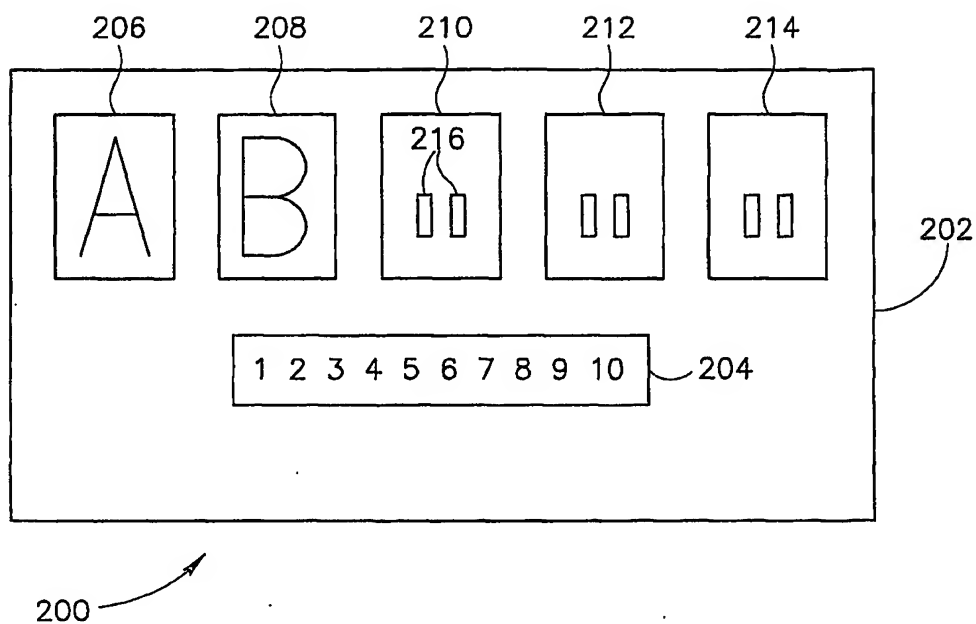


FIG. 2

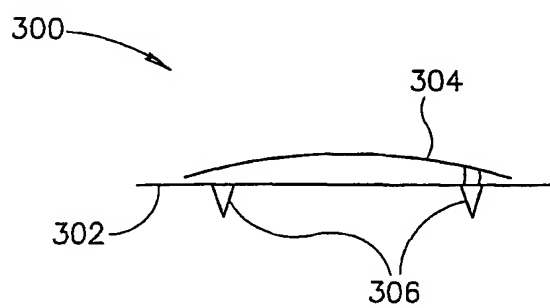


FIG. 3

3/7

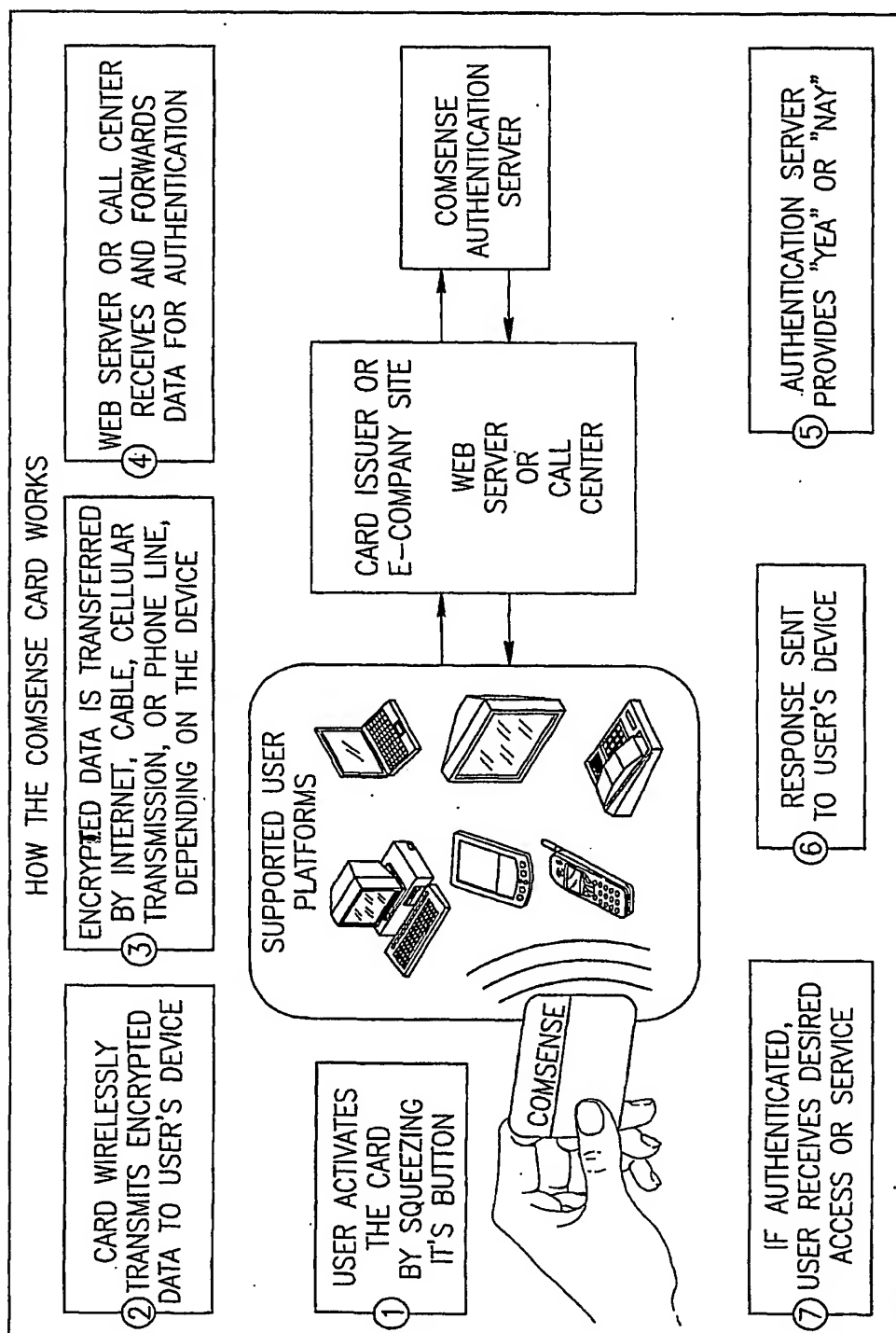


FIG.4

4/7

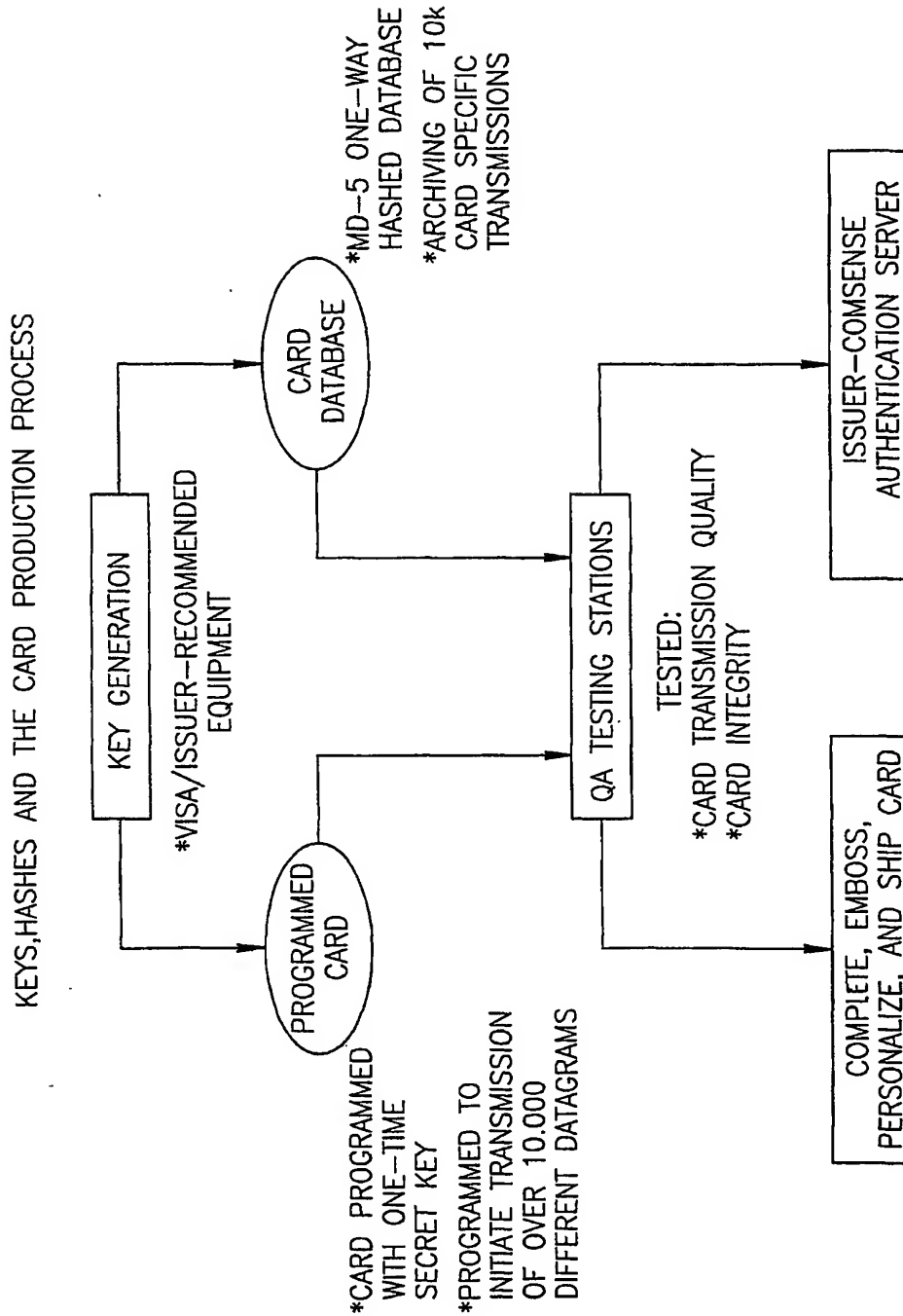


FIG.5

5/7

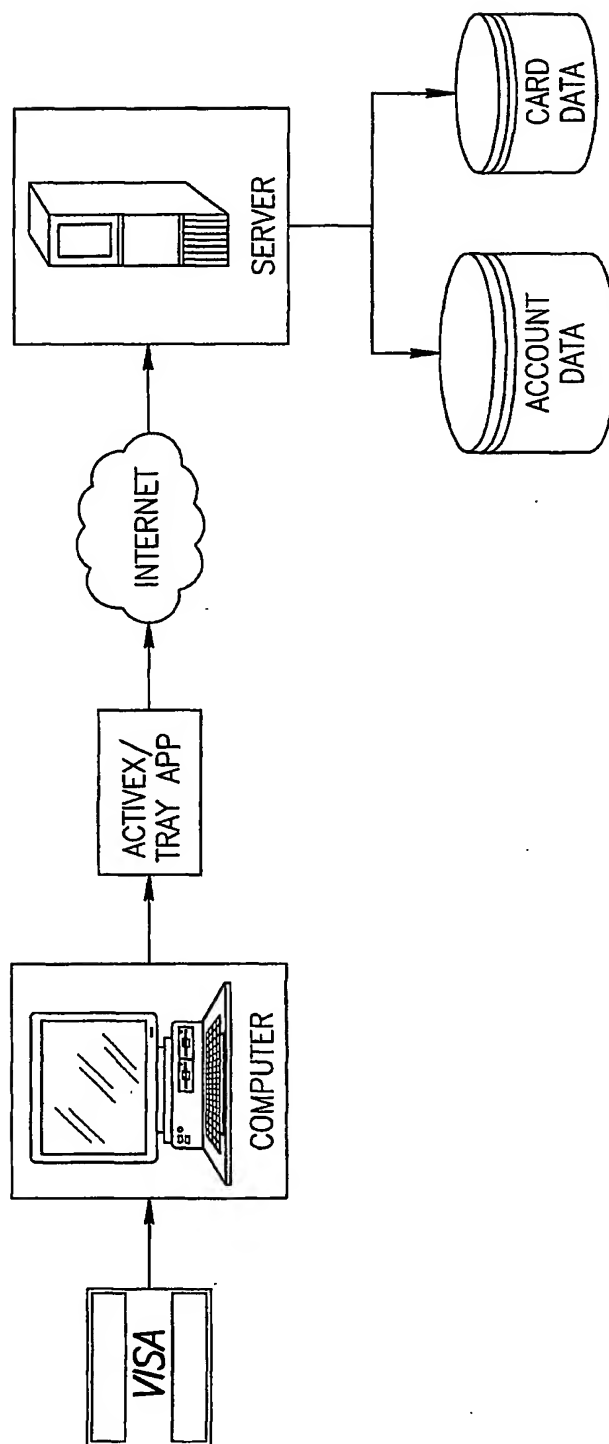


FIG.6

6/7

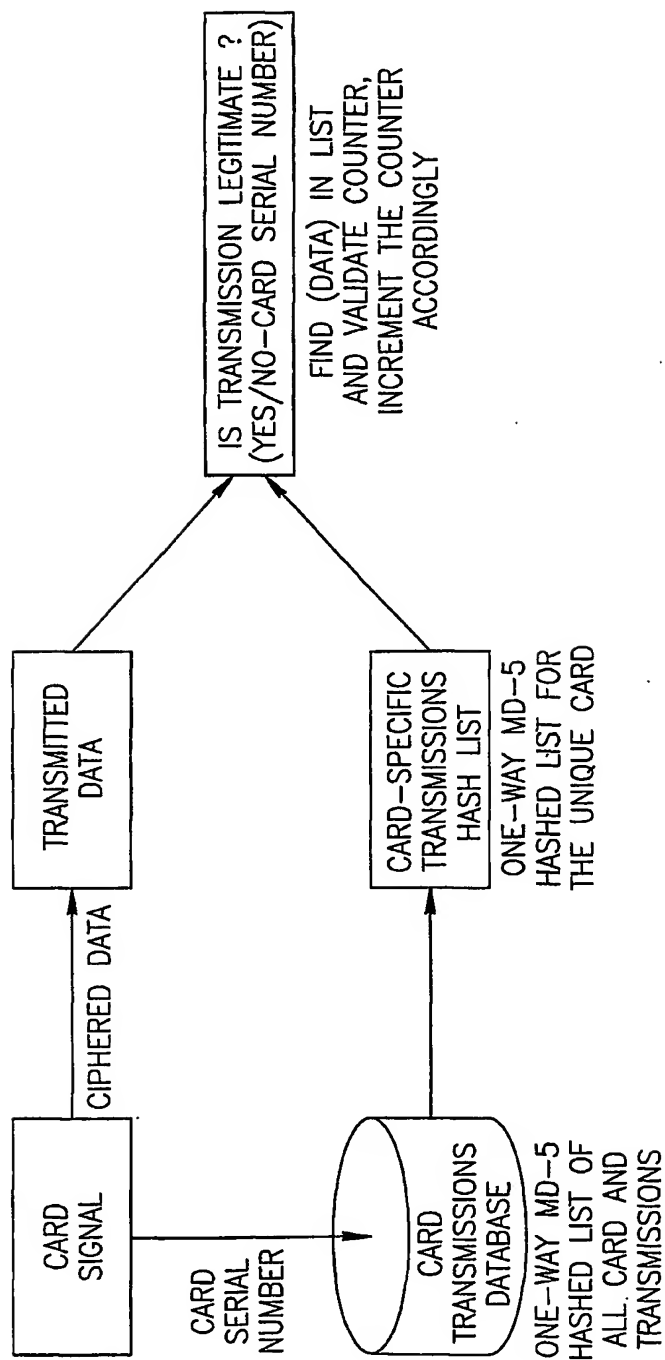


FIG. 7

7/7

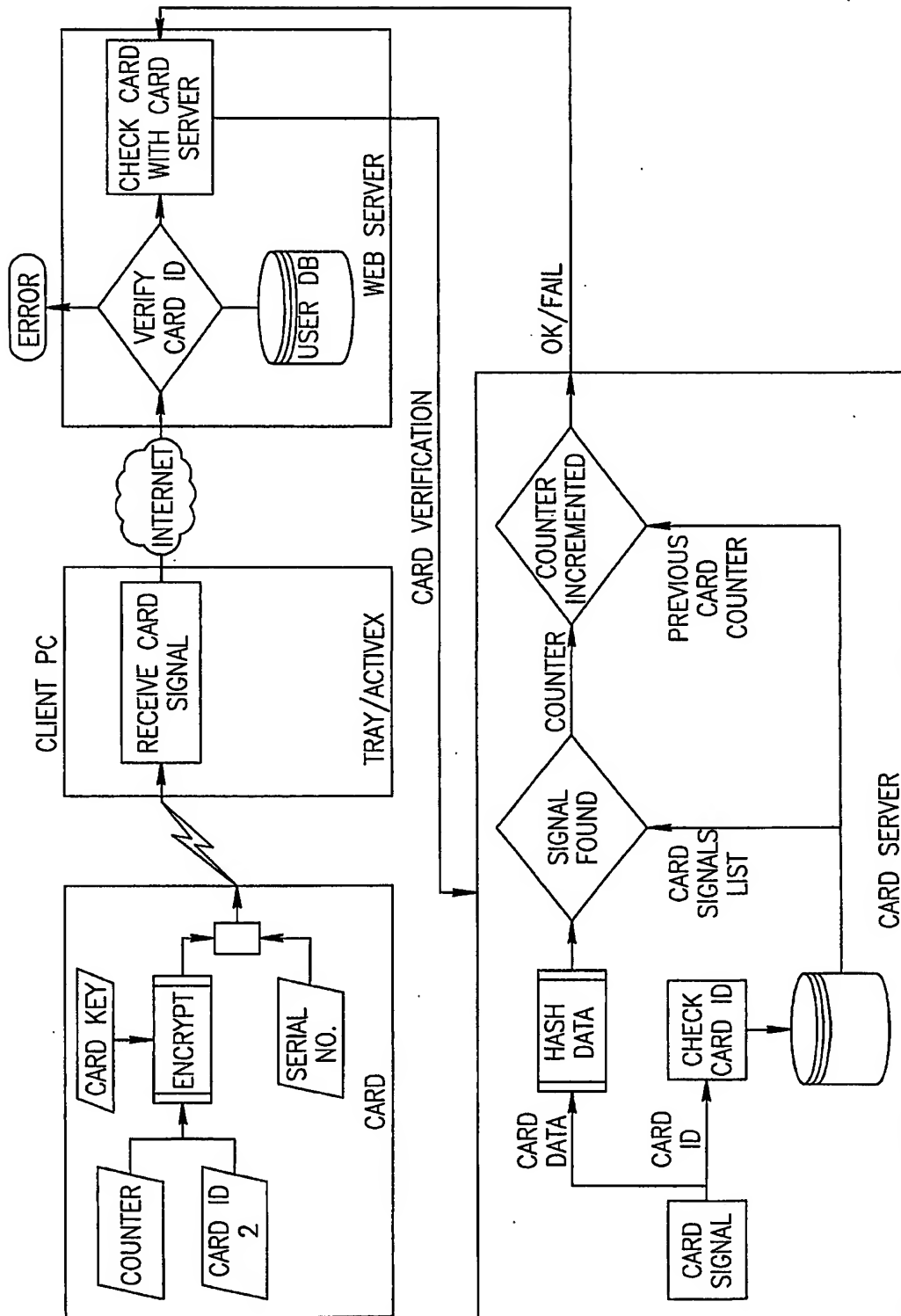


FIG.8